reading change data for changing the decrypting specifications;

automatically generating change data for changing the encrypting specification;

and

automatically changing a circuit structure of the at least one programmable logic device corresponding to the change data without removal of the at least one programmable logic device from the decrypting circuit.

25. (TWICE AMENDED) A signal processing method, comprising:

forming a circuit corresponding to given specifications with at least one programmable logic device; [and reading]

automatically generating change data for changing the specifications of the circuit, the specifications representing one of encrypting specifications or decrypting specifications[,]; and

reading the change data and automatically changing a structure of the circuit corresponding to the change data.

REMARKS

In the January 6, 2000 Office Action, the Examiner noted that claims 1-25 were pending in the application, rejected claims 21 and 22 under 35 U.S.C. § 102(b) and rejected claims 1-20 and 23-25 under 35 U.S.C. § 103(a). In rejecting the claims, U.S. Patents 4,972,478 to Dabbish; 5,703,950 to Jovanovich et al.; and 5,345,508 to Lynn et al. (References G, B and E, respectively in the March 23, 1999 Office Action) were cited. Claims 1-25 remain in the case. The Examiner's rejections are traversed below.

Rejection under 35 U.S.C. § 102(b)

In item 4 on page 2 of the January 6, 2000 Office Action, claims 21 and 22 were rejected under 35 U.S.C. § 102(b) as anticipated by Dabbish '478. All of the independent claims have been amended to add an element or process operation, e.g., "for automatically generating change data to change encrypting specifications" (claim 21, lines 4-5), or in the case of claim 22, "decrypting specifications" (claim 22, line 5). In the second paragraph of item 7, the Examiner acknowledged that "instructions to change the algorithm and the algorithm itself come from sources external to the circuit" (Detailed Action, fourth page, lines 2-3) in the circuit taught by Dabbish '478. Thus, claims 21 and 22 are not anticipated by Dabbish '478.

The lack of obviousness of the amended claims over Dabbish '478 will be discussed in the following section.

Rejections under 35 U.S.C. § 103(a)

In item 6 on page 3 of the Office Action, claims 1, 5, 8, 10, 14, 17, 19, 20 and 23-25 were rejected under 35 U.S.C. § 103(a) as unpatentable over Dabbish '478. As noted above, claims 21 and 22 will also be discussed in this rejection, since they have been amended to recite apparatuses that clearly are not anticipated by Dabbish '478. In addition, in item 8 claims 7 and 16 were also rejected under 35 U.S.C. § 103(a) as unpatentable over Dabbish '478.

As noted in item 2 on page 1 of the Office Action, the circuit disclosed by Dabbish '478 includes the ability to reprogram the crypto cores 100, 101 by using external programming equipment 105. The reference used to reject the claims, Dabbish '478 does not provide many details of the cryptographic cores 100, 101 but references U.S. Patent 4,914,697 to Dabbish et al. which describes a cryptographic apparatus which uses electronically erasable, programmable array logic (EEPAL) devices. Dabbish et al. '697 states that "an external device such as a microprocessor controlled computer is coupled to the address and data bus ports and is utilized to program the internal gate configurations of each EEPAL" (column 2, lines 64-67) after installation of the EEPAL. Initially, a test program is loaded and the device is delivered to a customer who "would then load the encryption device with the cipher algorithm by use of a similar external computer" (column 3, lines 5-7).

There is no suggestion in either Dabbish '478 or Dabbish et al. '697 that a device incorporating the circuits disclosed in these two patents include "a change data generating unit to generate **automatically** change data for changing at least one of the encrypting specifications" (claim 1, lines 5-6, emphasis added). As discussed in the Preliminary Amendment filed December 27, 1999, the "ability to automatically change circuit structure enables the present invention to provide the benefit of fast and flexible encryptions/decryption." Specifically, the present invention provides the benefit of a system that can apply many different algorithms to blocks of data that vary in length with encryption keys that vary in length and which does not require the user to be knowledgeable in encryption algorithms, nor does it require an external computer that has been programmed with encryption/decryption algorithms.

Claims 10 and 19-25 have been amended to recite limitation similar to those discussed above with respect to claim 1. Therefore, it is submitted that claims 1, 10 and 19-25, together

with claims 5, 7, 8, 14, 16 and 17 which depend from claims 1 and 10, patentably distinguish over Dabbish '478.

In item 7 on the third and fourth pages of the Detailed Action, claims 2-4, 6, 11-13 and 15 were rejected under 35 U.S.C. § 103(a) as unpatentable over Dabbish '478 in view of Jovanovich et al. Furthermore, in item 9 on the fifth and sixth pages of the Detailed Action, claims 9 and 18 were rejected under 35 U.S.C. § 103(a) as unpatentable over Dabbish '478 in view of Lynn et al. Since claims 2-4, 6, 9, 11-13, 15 and 18 depend from claims 1 and 10, it is submitted that these claims patentably distinguish over Dabbish '478 for the reasons discussed above with respect to claims 1 and 10. Furthermore, it is submitted that the addition of Jovanovich et al. or Lynn et al. does not overcome the deficiencies of Dabbish '478 discussed above, because as discussed in the December 27, 1999 Preliminary Amendment neither Jovanovich et al. or Lynn et al. teach or suggest automatically changing circuit structure without requiring knowledge of how to program an encryption algorithm in an external computer.

On the fourth page of the Detailed Action, column 3, lines 58-64 of Jovanovich et al. were cited as sufficient to make it obvious to a person of ordinary skill in the art "to store cipher algorithms in a database from which configuration means would compile an algorithm and write it, as an object, to the circuit" (lines 11-13). The cited portion of Jovanovich et al. begins a description of configuration data storage/processing unit 16 which includes "the frequency configuration data for all of the possible remote units ... [in] a database that stores data regarding the allowable operating frequencies for all of the countries in which the remote units may be operating" (column 3, lines 61-66). The mere fact that this frequency database is in a host computer that also "includes an encryption processing unit 14" (column 3, lines 58-59) does not provide sufficient suggestion to create an encryption algorithm database instead of a frequency database. The reason for providing the frequency database is to allow operation in many countries. The purpose of providing a change data generating unit as recited in the independent claims is to provide flexibility of encryption and decryption at a single location. The known practice of providing flexibility in operating frequencies by using a database is hardly a suggestion of automating the process of changing an encryption program. As repeatedly stated by the courts that hear appeals from the U.S. Patent Trademark Office, the prior art must contain some suggestion or incentive to make the modification. (See, e.g., In re Fritch, 23 USPQ2d 1784, 1781-1782 (Fed Cir. 1992), ACS Hospital Systems, Inc. v. Montefiore Hospital, 221 USPQ 929, 933 (Fed. Cir. 1984) and the cases cited therein). For

the above reasons, it is submitted that claims 2-4, 6, 11-13 and 15, as well as all of the independent claims patentably distinguish over Dabbish '478 in view of Jovanovich et al.

Similarly, the first paragraph of the Summary of the Invention section of Lynn et al. merely discloses modifying the pseudorandom number used as a temporal key in the encryption process. There is no suggestion of modifying the algorithm used to provide the type of flexibility provided by the present invention as discussed above. All of the statements in the cited portion of Lynn et al. are well known in the encryption art, i.e., the more often you change a pseudorandom number, the more difficult it is to detect the encryption technique used to generate encrypted data. However, this does not provide any suggestion that the technique used, i.e., the encryption and decryption algorithms, should be easily modified by including a change data component or processing operation. For the above reasons, it is submitted that claims 9 and 18, as well as all of the independent claims patentably distinguish over Dabbish '478 in view of Lynn et al.

Summary

It is submitted that the references cited by the Examiner, taken individually or in combination, do not teach or suggest the features of the present claimed invention. Thus, it is submitted that claims 1-25 are in a condition suitable for allowance. Entry of the Amendment, reconsideration of the claims and an early Notice of Allowance are earnestly solicited.

If any further fees are required in connection with the filing of this Amendment, please charge same to our Deposit Account No. 19-3935.

Respectfully submitted,

STAAS & HALSEY LLP

By: Richard A. Gollhofer
Richard A. Gollhofer
Registration No. 31,106

Suite 500
700 Eleventh St., N.W.
Washington, D.C. 20001
(202) 434-1500

Date: 4/6/00